Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, *et al*. *Plaintiffs*, v. BRAD RAFFENSPERGER, *et al.*, *Defendants*.	Civil Action No. 1:17-cv-2989-AT

CURLING PLAINTIFFS' FIRST REQUESTS FOR ADMISSION TO STATE DEFENDANTS

Pursuant to Federal Rules of Civil Procedure 26 and 36, Plaintiffs Donna Curling, Donna Price and Jeffrey Schoenberg (collectively, the "Curling Plaintiffs"), by and through counsel, hereby serve these First Requests for Admissions on State Defendants. Curling Plaintiffs requests that State Defendants answer these Requests fully in writing within fifteen (15) days of date of service pursuant to the agreed upon schedule (Dkt. No. 410-2).

DEFINITIONS

1. Curling Plaintiffs hereby incorporate by reference all definitions provided in the Curling Plaintiffs' June 3, 2019 Requests for Production of Documents and Inspection of Things to State Defendants, Plaintiffs' August 3, 2020

Joint Requests for Production of Documents and Inspection of Things to State Defendants, and Curling Plaintiff's July 9, 2021 Requests for Production of Documents and Inspection of Things to State Defendants.

2. "BMD System" shall mean the Election System adopted and implemented by Georgia in 2019, pursuant to the State's 2019 contract with Dominion Voting Systems.

3. "DRE System" shall mean the Election System used in Georgia immediately prior to the BMD System.

4. "GEMS System" shall mean all aspects of the Diebold system Microsoft Access database or databases used for programming, recording and reporting for Georgia elections, including the servers on which such databases are stored.

5. "Letter Report" shall mean the Letter Report regarding "Dominion Voting Systems ICX Version 5.5.10.32" from Pro V&V to Michael Barnes dated October 2, 2020 (Dkt. No. 939).

6. "Letter Report Software Change" shall mean the proposed code change by Dominion described in the Letter Report to address a flaw in the ICX software. "November 2020 Election" shall mean all local, state, and federal elections that took place in Georgia in November 2020 and shall include all early voting,

absentee voting, and in-person voting in such elections.

INSTRUCTIONS

1. These Requests shall be deemed to be continuing within the meaning of Federal Rule of Civil Procedure 26(e) with respect to any additional information which becomes known to State Defendants or their counsel up to and including the time of trial.

2. If you fail to respond or object to any request within 15 days of the service of the Requests, the matter shall be deemed admitted pursuant to the parties' agreement (Dkt. No. 410-2).

3. You must admit or deny each request, and, where necessary, specify the part(s) of each request to which you object or cannot in good faith admit or deny. If you object to only part of a Request, you must admit or deny the remainder of the Request. In the event that you object to or deny any Request or portion of a Request, you must state the reasons for your objection or denial.

4. If you answer a Request on the basis that you lack sufficient information to respond, you must describe any and all efforts you made to inform yourself of the facts and circumstances necessary to answer or respond.

5. If you do not admit an item, you shall: (i) produce to Curling Plaintiffs all documents regarding the Request in your possession, custody, or control; (ii) state, with particularity, the factual basis upon which your response is based; and

(iii) identify each and every person with knowledge of the Request for Admission.

6. Whenever necessary to bring within the scope of these Requests information that might otherwise be construed to be outside their scope, the singular shall include the plural, all references to the masculine shall include the feminine or neuter, and the disjunctive shall include the conjunctive, and vice versa. Furthermore, (a) the use of any verb in any tense shall be construed as the use of that verb in all other tenses; (b) the use of a word in its singular form shall be deemed to include within its use the plural form as well, and vice versa; and (c) the connectives "and" and "or" shall be construed either disjunctively or conjunctively.

7. In objecting to any Request herein, you shall identify the specific grounds for the objection, and shall state what information will be withheld in conjunction with that objection. If you object to part of any Request herein, you shall specify in the objection the part of the Request objected to, and shall respond to the remainder of the Request. If the objection is based on a claim of privilege or attorney work product, see the Instructions listed below.

8. If you object to or refuse to answer any Request on the basis that the answer reflects or would reveal the substance of a confidential or privileged communication, you shall: (i) state the nature of the privilege (including work product) being claimed; (ii) identify the person who made the communication, whether oral or in writing; (iii) if the communication was oral, identify all persons

present while the communication was made; (iv) if the communication was written, identify the author, addressees, and any other recipients; (v) identify the relationship of the author of the communication to each recipient; (vi) identify the relationship of the persons present to the person who made the communication; (vii) identify the date and place of the communication; (viii) describe the general subject matter of the communication; and (ix) provide any additional information necessary to enable the Court to adjudicate the propriety of that assertion.

9. If, in answering these Requests, you perceive any ambiguities in a Request, instruction, or definition, you shall set forth the matter deemed ambiguous and the construction used in answering.

10. These instructions, and the Definitions above, are incorporated into each of these Requests for Admission.

REQUEST FOR ADMISSIONS

1. Admit that Deputy Secretary of State Jordan Fuchs was not aware of any federal judge finding that Curling Plaintiffs have zero credibility when she made the following statement in in October 2020: "Other federal judges have more accurately found that these same activists and 'experts' who are spreading disinformation in Georgia have zero credibility."

2. Admit that You did not require all County Election Offices to furnish each precinct location with at least one printout of the voter registration list for that

precinct in every election after January 3, 2020.

3. Admit that You required all County Election Offices to furnish each precinct location with at least one printout of the voter registration list for that precinct in every election after January 3, 2020 as required by the Court in its August 15, 2019 Order.

4. Admit that You did not provide pre-election guidance to all County Election Offices regarding all polling officials' mandatory duty under law to provide voters the option of completing provisional ballots, including those who do not appear on the electronic voter registration database at a specific precinct or at all.

5. Admit that You provided pre-election guidance to all County Election Offices regarding all polling officials' mandatory duty under law to provide voters the option of completing provisional ballots, including those who do not appear on the electronic voter registration database at a specific precinct or at all as required by the Court in its August 15, 2019 Order.

6. Admit that You did not prominently post information concerning the casting of provisional ballots and voters' submission of additional information, including their registration status, and voters' capacity to check the status of their provisional ballot on the SOS website throughout the course of any state or federal elections.

7. Admit that You prominently posted information concerning the

casting of provisional ballots and voters' submission of additional information, including their registration status, and voters' capacity to check the status of their provisional ballot on the SOS website throughout the course of any state or federal elections as required by the Court in its August 15, 2019 Order.

8. Admit that the Secretary of State's Office did not work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of the Election System.

9. Admit that the Secretary of State's Office did not work with a consulting cybersecurity firm to conduct a non-privileged in-depth review and formal assessment of the Election System.

10. Admit that You did not produce any reports containing the substance of any work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of the Election System.

11. Admit that You did not produce any in-depth review or formal assessment of the Election System required by the Court in its August 15, 2019 Order.

12. Admit that the Secretary of State's Office did not work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of the Election System after August 15, 2019.

13. Admit that the Secretary of State's Office did not work with a

consulting cybersecurity firm to conduct a non-privileged in-depth review and formal assessment of the Election System after August 15, 2019.

14. Admit that You did not produce to Plaintiffs any reports containing the substance of any work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of the Election System after August 15, 2019.

15. Admit that You did not produce to Plaintiffs any in-depth review or formal assessment of the Election System required by the Court in its August 15, 2019 Order.

16. Admit that the Secretary of State's Office did not work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of the BMD System.

17. Admit that the Secretary of State's Office did not work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of the BMD System after August 15, 2019.

18. Admit that the Secretary of State's Office did not work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of issues relating to exposure of the voter registration database.

19. Admit that the Secretary of State's Office did not work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of issues relating to accuracy of the voter registration database.

20. Admit that the Secretary of State's Office did not work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of issues relating to the State's database or handling of the EPoll voter database and function.

21. Admit that the Secretary of State's Office did not work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of issues relating to exposure of the voter registration database after August 15, 2019.

22. Admit that the Secretary of State's Office did not work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of issues relating to accuracy of the voter registration database after August 15, 2019.

23. Admit that the Secretary of State's Office did not work with a consulting cybersecurity firm to conduct an in-depth review and formal assessment of issues relating to the State's database or handling of the EPoll voter database and function after August 15, 2019.

24. Admit that You did not file with the Court all proposed and final audit requirements that the State Elections Board and Secretary of State's Office considered or approved in connection with elections held in 2020 or thereafter.

25. Admit that You did not develop procedures or take other action to address all the deficiencies found by the Court in its August 15, 2019 Order concerning the Election System.

26. Admit that You did not develop procedures or take other action to address all the deficiencies found by the Court in its August 15, 2019 Order concerning the voter registration database.

27. Admit that You did not develop procedures or take other action to address any of the deficiencies found by the Court in its August 15, 2019 Order concerning the voter registration database.

28. Admit that You did not develop procedures to address all the deficiencies found by the Court in its August 15, 2019 Order concerning the ExpressPoll system.

29. Admit that You did not develop procedures to address any of the deficiencies found by the Court in its August 15, 2019 Order concerning the ExpressPoll system.

30. Admit that You did not develop a plan for implementation prior to January 3, 2020 that addressed the procedures to be undertaken by election officials to address errors and discrepancies in the voter registration database that may cause eligible voters to not appear as eligible voters in the electronic pollbooks.

31. Admit that You did not develop a plan for implementation prior to January 3, 2020 that addressed the procedures to be undertaken by election officials to address errors and discrepancies in the voter registration database that may cause eligible voters to receive the wrong ballot.

32. Admit that You did not develop a plan for implementation prior to January 3, 2020 that addressed the procedures to be undertaken by election officials to address errors and discrepancies in the voter registration database that may cause eligible voters to be assigned to the wrong precinct in the electronic pollbook.

33. Admit that You did not develop a plan for implementation prior to January 3, 2020 that addressed the procedures to be undertaken by election officials to address errors and discrepancies in the voter registration database that may cause eligible voters to be prevented from casting a regular ballot in their properly assigned precinct.

34. Admit You did not produce to Plaintiffs a copy of a plan for implementation as described in paragraph 1 of the Court's August 15 2019 Order at p. 149.

35. Admit that the bootloader software used in the DREs used for Georgia elections was not updated for over eighteen years.

36. Admit that the Secretary of State's Office did not update the bootloader software used in the DREs used for Georgia elections for over eighteen years.

37. Admit that the BallotStation election software installed on the DREs used for Georgia elections was not updated for over thirteen years.

38. Admit that the Secretary of State's Office did not update the

BallotStation election software installed on the DREs used for Georgia elections for over thirteen years.

39. Admit that all the memory cards and DREs used for Georgia elections used the same default encryption key, F26554hD4, that was installed on the AccuVote DREs at the factory.

40. Admit that You are not aware of the default encryption key, F26554hD4, that was installed on the AccuVote DREs at the factory being changed for all the memory cards and DREs used for Georgia elections after receiving that equipment from the manufacturer.

41. Admit that You are not aware of the default encryption key, F26554hD4, that was installed on the AccuVote DREs at the factory being changed for any of the memory cards and DREs used for Georgia elections after receiving that equipment from the manufacturer.

42. Admit that the State did not change the default encryption key used in all memory cards and DREs used for Georgia elections for over 17 years.

43. Admit the DRE System is completely separate from the BMD System.

44. Admit the DRE System is not completely separate from the BMD System.

45. Admit the BMD System uses some components from the DRE System.

46. Admit the BMD System uses some data from the DRE System.

47. Admit the BMD System has at some point used some components from the DRE System.

48. Admit the BMD System has at some point used some data from the DRE System.

49. Admit that one or more removable media used with the DRE system have at some point been used with the BMD System.

50. Admit that one or more removable media connected at some point to one or more components of the DRE System have at some point been connected to one or more components of the BMD System.

51. Admit that the BMD System is not completely separate from the eNet System.

52. Admit the BMD System uses some components from the eNet System.

53. Admit the BMD System uses some data from the eNet System.

54. Admit the BMD System has at some point used some components from the eNet System.

55. Admit the BMD System has at some point used some data from the eNet System.

56. Admit that one or more removable media used with the eNet System have at some point been used with the BMD System.

57. Admit that one or more removable media connected at some point to one or more components of the eNet System have at some point been connected to one or more components of the BMD System.

58. Admit that the DRE System was not completely separate from the eNet system.

59. Admit the DRE System uses some components from the eNet System.

60. Admit the DRE System uses some data from the eNet System.

61. Admit the DRE System has at some point used some components from the eNet System.

62. Admit the DRE System has at some point used some data from the eNet System.

63. Admit that one or more removable media used with the eNet System have at some point been used with the DRE system.

64. Admit that one or more removable media connected at some point to one or more components of the eNet System have at some point been connected to one or more components of the DRE system.

65. Admit that security deficiencies or vulnerabilities identified by Fortalice with the eNet System have not been fully mitigated.

66. Admit that in some jurisdictions in Georgia, the same County IT infrastructure is being used to copy data in and out of the new Dominion EMS system

as was used with the GEMS System.

67. Admit that the eNet voter registration database system used with the DRE System was used in elections after January 1, 2020.

68. Admit that PCC, including its successors, subsidiaries, or affiliates, hosted or operated eNet after January 1, 2020.

69. Admit that PCC, including its successors, subsidiaries, or affiliates, continues to host or operate eNet.

70. Admit that PCC, including its successors, subsidiaries, or affiliates, continues to develop or maintain the eNet software.

71. Admit that the same thumb drives were used multiple times to copy results from GEMS System to the ENR System during the November 2020 Election.

72. Admit that technicians working for or at the direction of Dominion used remote access tools to access election management systems in preparation for the November 2020 Election.

73. Admit that technicians working for or at the direction of Dominion used remote access tools to access election management systems during the November 2020 Election.

74. Admit there was no systematic method of tracking the number of Georgia voters that complained that the BMD printout for their respective votes did not match the selections they each made on the corresponding BMD in the

November 2020 Election.

75. Admit that there is no comprehensive collection or record of complaints or reports from Georgia voters that the BMD printout for their respective votes did not match the selections they each made on the corresponding BMD in the November 2020 Election.

76. Admit that the November 2020 election for president was followed by a full hand recount of the human-readable text on all ballots, including the BMD-marked ballots and hand-marked paper ballots.

77. Admit that the results of the full hand recount of the human-readable text on BMD-marked ballots matched the results of the QR Code scanning for those ballots within an expected margin of error.

78. Admit that the results of the full hand recount of the human-readable text on BMD-marked ballots did not match the results of the QR Code scanning for those ballots within an expected margin of error.

79. Admit that the "audit" performed in connection with the November 2020 Election did not check the accuracy of the vote count or election results of any race other than the Presidential election.

80. Admit that the full hand recount performed in connection with the November 2020 Election did not check whether the human-readable text on BMD-marked ballots matched the results of the QR Code scanning.

81. Admit that the full hand recount performed in connection with the November 2020 Election did not check whether the human-readable text on BMD-marked ballots actually reflected the selections each voter intended for each of those ballots.

82. Admit that the full hand recount performed in connection with the November 2020 Election did not check whether the QR codes on BMD-marked ballots actually reflected the selections each voter intended for each of those ballots.

83. Admit that You have not adopted specific measures to verify and confirm that the human-readable text on BMD-marked ballots actually reflects the selections each voter intended for each such ballot in Georgia elections.

84. Admit that You have not commissioned, conducted, undertaken, or directed any studies or research to evaluate the ability of voters to reliably review the human-readable text on their respective BMD-marked ballots to determine whether their respective ballots actually reflect each and every selection the voter intended for each such ballot.

85. Admit that You have not commissioned, conducted, undertaken, or directed any studies or research to evaluate the willingness of voters to carefully review the human-readable text on their respective BMD-marked ballots to determine whether their respective ballots actually reflect each and every selection the voter intended for each such ballot.

86. Admit that You have not commissioned, conducted, undertaken, or directed any studies or research the evaluate the ability of voters to reliably review the human-readable text on their respective BMD-marked ballots to determine whether those ballots actually reflect each and every selection the voter made on the corresponding BMD for each such ballot.

87. Admit that You have not commissioned, conducted, undertaken, or directed any studies or research the evaluate the willingness of voters to carefully review the human-readable text on their respective BMD-marked ballots to determine whether those ballots actually reflect each and every selection the voter made on the corresponding BMD for each such ballot.

88. Admit that voters cannot read QR codes on their respective BMD-marked ballots to determine whether their respective ballots actually reflect each and every selection the voter made on the corresponding BMD for each such ballot.

89. Admit that the technicians who installed the software update in October 2020 followed the instructions provided by the State exactly.

90. Admit that the hash value comparison as performed during acceptance testing is insufficient to verify the integrity of all software components running on the BMD.

91. Admit that the hash value comparison as performed during installation of the October 2020 software update is insufficient to verify the integrity of some

software components running on the BMD.

92. Admit that the hash value comparison performed by Pro V&V in November 2020 is insufficient to verify the integrity of some software components running on the BMD.

93. Admit that the USB cable attached to the BMD is not sealed to the laser printer.

94. Admit that the 22 vulnerabilities Fortalice identified in the Secretary of State's information technology environment have not been fully remediated.

95. Admit that You have not performed a comprehensive cybersecurity analysis of the Election System.

96. Admit that You have not produced in discovery a comprehensive cybersecurity analysis of the Election System.

97. Admit that You have not engaged an independent cybersecurity expert to analyze the security and vulnerabilities of the Election System.

98. Admit that Fortalice has not generated any consulting studies, audits, reports, or assessments of data issues since August 1, 2019, other than a November 2019 report withheld based on attorney-client privilege.

99. Admit that You have never checked that the QR codes matched the human readable portion of the text for a BMD-generated ballot in a Georgia election.

100. Admit that You have no procedures in place to check that the QR

codes match the human readable text of voter ballots.

101. Admit that You are aware of attack attempts against election-related computer systems in Georgia.

102. Admit that the election definition files are created by Dominion or subcontract employees and not State employees.

103. Admit that the State has no ability to verify the security of the systems used to create election definition files.

104. Admit that the State does not know what security measures Pro V&V takes in creating software images for the election system.

105. Admit that BMD printed ballots that are photocopied are counted the same as originals by the scanner equipment.

106. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined each BMD used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

107. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined any BMD used in any actual elections in Georgia to determine whether malware was loaded on to any such BMD at any point in time.

108. Admit that no consultant or vendor engaged by you at any time has, to

your knowledge, forensically examined each BMD used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

109. Admit that no consultant or vendor engaged by you at any time has, to your knowledge, forensically examined any BMDs used in any actual elections in Georgia to determine whether malware was loaded on to any such BMD at any point in time.

110. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine any BMDs used in any actual elections in Georgia to determine whether malware was loaded on to any such BMD at any point in time.

111. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine each BMD used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

112. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined any BMDs configured identically to machines used in Georgia elections.

113. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined each printer used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

114. Admit that no expert who has testified on your behalf in this litigation

has, to your knowledge, forensically examined any printer used in any actual elections in Georgia to determine whether malware was loaded on to any such printer at any point in time.

115. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined each printer used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

116. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined any printers used in any actual elections in Georgia to determine whether malware was loaded on to any such printer at any point in time.

117. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine any printer used in any actual elections in Georgia to determine whether malware was loaded on to any such printer at any point in time.

118. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine each printer used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

119. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined any printers configured identically to machines used in Georgia elections.

120. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined each scanner used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

121. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined any scanner used in any actual elections in Georgia to determine whether malware was loaded on to any such scanner at any point in time.

122. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined each scanner used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

123. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined any scanner used in any actual elections in Georgia to determine whether malware was loaded on to any such scanner at any point in time.

124. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine any scanner used in any actual elections in Georgia to determine whether malware was loaded on to any such scanner at any point in time.

125. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine each scanner used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

126. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined any scanners configured identically to machines used in Georgia elections.

127. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined each USB device used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

128. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined any USB device used in any actual elections in Georgia to determine whether malware was loaded on to any such printer at any point in time.

129. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined each USB device used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

130. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined any USB device used in any

actual elections in Georgia to determine whether malware was loaded on to any such printer at any point in time.

131. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine any USB device used in any actual elections in Georgia to determine whether malware was loaded on to any such printer at any point in time.

132. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine each USB device used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

133. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined each server, including EMS server, used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

134. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined any server, including EMS server, used in any actual elections in Georgia to determine whether malware was loaded on to any such server at any point in time.

135. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined each server, including EMS server, used in any actual elections in Georgia to determine whether malware was

loaded on to it at any point in time.

136. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined any server, including EMS server, used in any actual elections in Georgia to determine whether malware was loaded on to any such server at any point in time.

137. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine any server, including EMS server, used in any actual elections in Georgia to determine whether malware was loaded on to any such server at any point in time.

138. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine each server, including EMS server, used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

139. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined the eNet Voter registration system used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

140. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined the eNet Voter registration system used in any actual elections in Georgia to determine whether malware was

loaded on to it at any point in time.

141. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine any eNet Voter registration system used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

142. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined each voter registration database used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

143. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined any voter registration database used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

144. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined each voter registration database used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

145. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined any voter registration database used in any actual elections in Georgia to determine whether malware was loaded

on to it at any point in time.

146. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine any voter registration database used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

147. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine each voter registration database used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

148. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined each KnowInk PollPad used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

149. Admit that no expert who has testified on your behalf in this litigation has, to your knowledge, forensically examined any KnowInk PollPad used in any actual elections in Georgia to determine whether malware was loaded on to any such Pad at any point in time.

150. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined each KnowInk PollPad used in any actual elections in Georgia to determine whether malware was loaded on to it at

any point in time.

151. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined any KnowInk PollPad used in any actual elections in Georgia to determine whether malware was loaded on to any such Pad at any point in time.

152. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine any KnowInk PollPad used in any actual elections in Georgia to determine whether malware was loaded on to any such Pad at any point in time.

153. Admit that you have not directed any person, consultant, or vendor at any time to forensically examine each KnowInk PollPad used in any actual elections in Georgia to determine whether malware was loaded on to it at any point in time.

154. Admit that no person, consultant, or vendor engaged by you at any time has, to your knowledge, forensically examined any KnowInk PollPad configured identically to machines used in Georgia elections.

155. Admit that Pro V&V has never performed penetration testing of the Election System.

156. Admit that the State has not tested whether the State's procedures cause voters to reliably spot errors on their BMD printed ballots.

157. Admit that you do not know whether each printed ballot generated by

a Dominion BMD in any actual election in Georgia actually correctly captured the corresponding voter's intent for each selection appearing on that printed ballot.

158. Admit that you do not know whether each printed ballot generated by a Dominion BMD in any actual election in Georgia actually correctly captured the corresponding voter's selections made on that BMD for each selection appearing on that printed ballot.

159. Admit that you do not know whether the majority of printed ballots generated by Dominion BMDs in any actual election in Georgia actually correctly captured the corresponding voters' intent for each selection appearing on those printed ballots.

160. Admit that you do not know whether the majority of printed ballots generated by Dominion BMDs in any actual election in Georgia actually correctly captured the corresponding voters' selections made on those BMDs for each selection appearing on those printed ballots.

161. Admit that you do not know whether each voter who voted on a Dominion BMD in any actual election in Georgia actually reviewed and confirmed the accuracy of the printed ballot generated for and cast by that voter in the corresponding election.

162. Admit that you do not know whether the majority of voters who voted on Dominion BMDs in any actual election in Georgia actually reviewed and

confirmed the accuracy of the printed ballots generated for and cast by those voters in the corresponding election.

163. Admit that Pro V&V never performed a security analysis of the Dominion voting system version deployed in Georgia.

164. Admit that Pro V&V never performed penetration testing of the Dominion voting system deployment in Georgia.

165. Admit that Pro V&V never performed penetration testing that examined every component of the Dominion voting system deployment in Georgia.

166. Admit that since the November 2020 Election, Pro V&V examined fewer than 30 pieces of election equipment across the state.

167. Admit that the hash checks that Pro V&V performed in November 2020 did not examine all software resident on the BMD.

168. Admit that the hash checks that Pro V&V performed in November 2020 did not examine all software resident on the EMS.

169. Admit that the hash checks that Pro V&V performed in November 2020 did not examine all software resident on the ICP.

170. Admit that the hash checks that Pro V&V performed in November 2020 did not examine all software resident on the ICC.

171. Admit that the counties where Pro V&V performed the hash checks in in November 2020 knew they would be audited before the auditors arrived.

172. Admit that the Georgia Secretary of State selected the counties where Pro V&V performed the hash checks in November 2020.

173. Admit that the testing relating to the "Letter Report" prepared by Pro V&V concerning version 5.5.10.32 of the Dominion BMD software (Dkt. No. 939) did not attempt to independently verify the cause of the ballot display problem.

174. Admit that the testing relating to the "Letter Report" did not verify that the changes were an effective solution.

175. Admit that the testing relating to the "Letter Report" did not test whether the changes created new problems impacting the reliability, accuracy, or security of the BMD system.

176. Admit that the testing relating to the "Letter Report" did not test the security of the system.

177. Admit the testing relating to the "Letter Report" was not a comprehensive test of the Dominion BMD software.

178. Admit the testing relating to the "Letter Report" did not consider whether the Letter Report Software Change negatively impacted the functionality of the voting system.

179. Admit the testing relating to the "Letter Report" did not comprehensively test whether the Letter Report Software Change negatively impacted the functionality of the voting system.

180. Admit the Letter Report Software Change was not a one-line configuration change.

181. Admit the Letter Report Software Change was not a configuration change.

182. Admit the Letter Report Software Change modified lines in five different source code files.

183. Admit that the systems that Pro V&V used to test the election software were not NIST 800-171 compliant.

184. Admit that Pro V&V has never had a security audit performed by a third party of the systems used to test the election software.

185. Admit that you have no evidence that no malware was actually inserted into any component of the Election System prior to or during the elections held on November 3, 2020.

186. Admit that you have no evidence of any widespread voter fraud in Georgia in connection with the elections held in Georgia on November 3, 2020 and January 5, 2021.

187. Admit that there were no malfunction(s) of any component of the Election system for the election held in Georgia on November 3, 2020.

188. Admit that you have no evidence that the Election System failed to count any legal vote(s) in the election held on November 3, 2020.

189. Admit that you have no evidence that the Election System counted any illegal vote(s) in the election held on November 3, 2020.

190. Admit that you have no evidence that there was any mismatch between the QR Codes on the Paper Ballots cast in the November 3, 2020 election and the human-readable portion of the Paper Ballots, individually or in total.

191. Admit that you have evidence that there was a mismatch, however small, between the QR Codes on the Paper Ballots cast in the November 3, 2020 election and the human-readable portion of the Paper Ballots, individually or in total.

Dated: October 29, 2021

Respectfully submitted,

/s/ David D. Cross
David D. Cross (*pro hac vice*)
Veronica Ascarrunz (*pro hac vice*)
Lyle P. Hedgecock (*pro hac vice*)
Mary G. Kaiser (*pro hac vice*)
Robert W. Manoso (*pro hac vice*)
MORRISON & FOERSTER LLP
2100 L St, NW
Washington, DC
Telephone: (202) 887-1500
DCross@mofo.com
VAscarrunz@mofo.com
LHedgecock@mofo.com
MKaiser@mofo.com
RManoso@mofo.com

Halsey G. Knapp, Jr.
GA Bar No. 425320
Adam M. Sparks
GA Bar No. 341578

KREVOLIN & HORST, LLC
1201 West Peachtree Street, NW
Suite 3250
Atlanta, GA 30309
HKnapp@khlawfirm.com
Sparks@khlawfirm.com

Counsel for Plaintiffs Donna Curling, Donna Price & Jeffrey Schoenberg

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF SERVICE

I hereby certify that on October 29, 2021, a copy of the foregoing **CURLING PLAINTIFFS' FIRST REQUESTS FOR ADMISSION TO STATE DEFENDANTS** was served on all counsel of record by electronic delivery of a PDF version.

/s/ David D. Cross
David D. Cross